A Novel Approach for Video Hashing

Jitendra Singh Chauhan - Research Scholar, Pacific University, Pacific Hills Udaipur (Rajasthan), India

S. K. Sharma - Research Guide, Pacific University, Pacific Hills Udaipur (Rajasthan), India

Abstract: Secure image and video transmission over network is a crucial issue these days, due to the rapid growth of highly secure data needs. As, the major concern regarding the copyright protection of videos increase as the users of consumers electronics shares tens of thousands of videos every day. This paper proposes a novel method for video hashing for copyright protection, media monitoring, etc. The proposed method is applied to temporally representative images of a video and its robustness is found with respect to several distortions like noise, changes in colour, brightness, temporal shift, spatial shift, etc. and the results shows that the proposed method is effective and robust.

Key Words: Copy right protection, Temporally representative image (TRI), Hashing, Video objects, Frames, Confusion, Diffusion.

Introduction:

There are many aspects to security and many applications, ranging from secure transmission of data, protecting passwords, On-line security, On-line banking and many more[2]. Data encryption comes under the category of mathematical applications in terms of information security, which incorporates the management and manipulation of data [1]. One essential aspect for secure communications is cryptography which can be defined as the conversion of data into a ciphered code that can be deciphered and also could be safely send across a public or private network. Alone Cryptography it is not sufficient for secure transmission of information [1] [5].

The copyright protection for the security of videos is a major concern with the rapid growth of video sharing websites. Watermarking technique is somehow feasible for image encryption but for video communication watermarking is not feasible as it requires extra information to be inserted which is not practically feasible at the sender side as it increases cost of computation while searching [1] [5] [8].

Video hashing is still in its preliminary research phase and the currently available video hashing approaches are based on extending the expansion of current hashing algorithms for still images but these approaches are sensitive to frame dropping and noise. So paper has devised a method which incorporates the temporal information derived from video sequence and provides the image hash with both the spatial and temporal information of the video sequence [1] [2] [4].

Digital Marketing:

The copyright protection for the security of videos is a major concern with the rapid growth of video sharing websites. Watermarking technique is somehow feasible for image encryption but for video communication watermarking is not feasible as it requires extra information to be inserted which is not practically feasible at the sender side as it increases cost of computation while searching [1] [5] [8].

Video hashing is still in its preliminary research phase and the currently available video hashing approaches are based on extending the expansion of current hashing algorithms for still images but these approaches are sensitive to frame dropping and noise. So paper has devised a method which incorporates the temporal

information derived from video sequence and provides the image hash with both the spatial and temporal information of the video sequence [1] [2] [4].

Finger printing:

A fingerprint is a content based signature derived from a multimedia asset so that it specifically represents that asset. Robustness and uniqueness are the two essential properties for a video fingerprint to be efficient and effective [6] [7]. Another important requirement is the complexity i.e. the less complex the more efficient is the fingerprint system.

Cano et al. [7] have listed some additional requirements with respect to video fingerprint like accuracy, reliability, granularity, security, versatility, scalability, fragility.

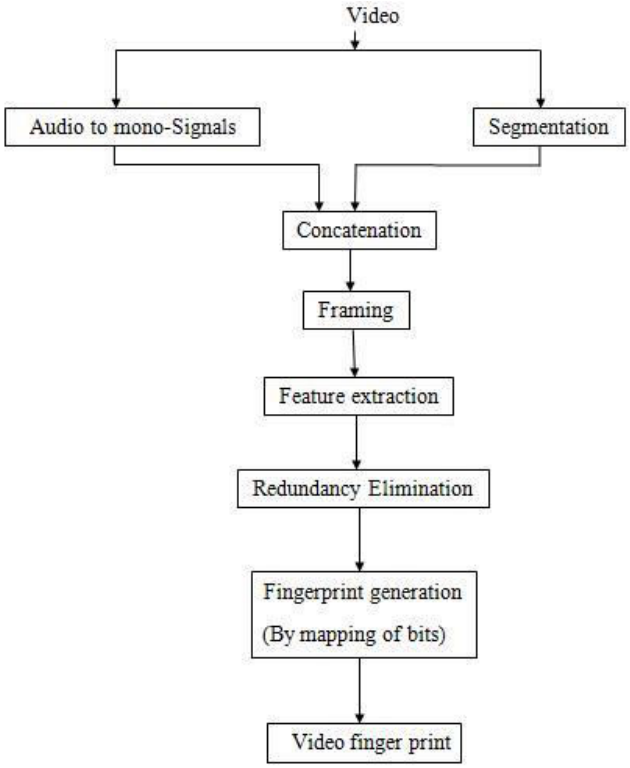

Figure 1.1 General frame work of video fingerprinting

Proposed Method and Hypothesis:

In order to generate a secure hash for video objects various methods could be used but none of them could be highly effective, efficient and robust. This section gives the description of the proposed hashing approach.

The following assumptions have been taken into consideration:

- Firstly the video sequence is divided into video segments of fixed length which incorporates the temporal information also.
- The spatial resizing and time re-sampling of video objects is done into fixed W x H x F pixels/second, W x H denotes frame size (W for width and H for height) and F denotes frame rate.
- TRI segmentation is done into N x N size blocks and horizontal features (α_1, α_2, ……..…….α_n) and vertical features (β_1, β_2, …….β_n) are extracted from it.

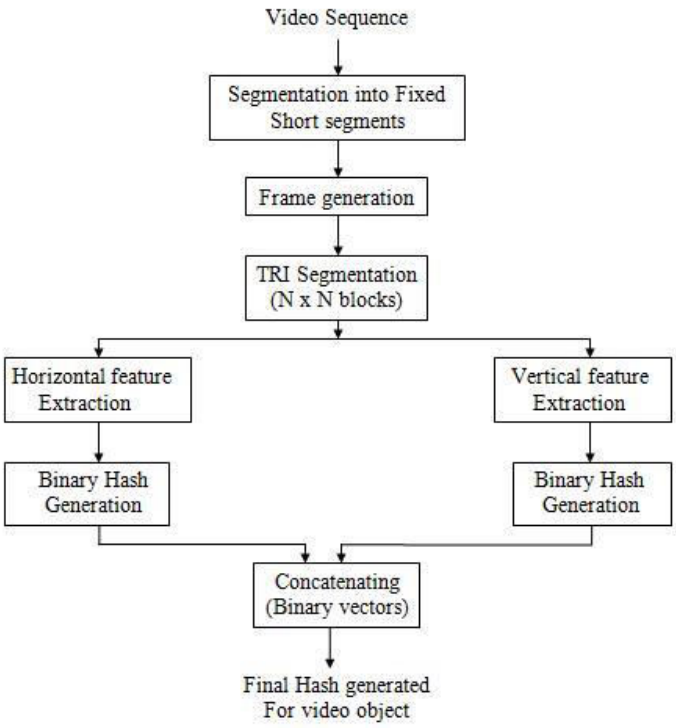

FIGURE 1.2 PROPOSED FRAME WORK OF VIDEO HASHING

$$\alpha = \sum_{y=1}^{N}\sum_{x=1}^{N} l_{x,y} \cos(3.14\,(x+0.5)/Z)$$

$$\beta = \sum_{x=1}^{N}\sum_{y=1}^{N} l_{x,y} \cos(3.14\,(x+0.5)/Z)$$

Then TRI is generated for each segment. Let $l_{x,\,y,\,n}$ be the luminance value of the $(x, y)^{th}$ pixel of the n^{th} frame.

$$V_{x,y} = \sum_{t=1}^{N} \alpha^t \beta^t l_{x,y,t}$$

- To generate the binary hash for horizontal feature extracted, each coefficient is replaced by 0 if it is less than the median values of all the coefficients and 1 otherwise. In the same way binary hash of vertical feature is also calculated.
- Concatenate Horizontal and Vertical binary hash to generate the final binary hash of video objects.

V. SIMULATION RESULTS

We ran the simulations on training set of videos taken from ocean [9] were used. We choose β= 0.5, α = 0.5 and Z = 32 pixels with 60% overlapping between adjacent blocks. Then some attacks like noise, rotation, frame dropping, etc. are mounted. Then the generated hash of TIRI – DCT, TIRI – DCT & DWT and Proposed versions are compared with each other to check the correctness (copy right protection) of video objects. True positive rate (TPR) and False Positive rate (FPR) of the algorithms are computed as, shown in Table 1. All the three algorithms are robust against changes in brightness and contrast but the proposed algorithm is more robust to many of the other attacks like increase in noise and frame drop.

The proposed algorithm is slightly less robust against geometric attacks like rotation and shift (but these attacks degrade the perceptual quality of videos and make them unusable).

Security Attacks	Proposed Algorithm		TIRI - DCT		TITI – DCT & DWT	
	TPR (%)	FPR (%)	TPR (%)	FPR (%)	TPR (%)	FPR (%)
Brightness	99.41	0.70	99.40	0.60	99.42	0.67
Noise	99.32	0.68	99.24	0.66	99.26	0.67
Contrast	99.11	0.80	99.00	0.75	99.10	0.80
Frame drop (about 50 %)	99.4	0.40	98.3	0.40	98.4	0.51
Rotate by 5 degree	97.9	0.60	55.10	0.82	97.5	0.70
Spatial shift by 5 pixels	80.00	0.71	57.1	0.75	81.4	0.74

TABLE 1 PERFORMANCE COMPARISON OF THE ALGORITHMS

Conclusion and Future work:

The video copy detection is a crucial issue these days to the video sharing websites. The paper has proposed an algorithm which uses the strengths of TIRI – DCT, TIRI – DCT & DWT algorithms and allows more secure and robust method for video hashing. Simulations run on a database of 100 videos shows the high discriminating ability of the algorithm. As, part of future work, we can extend performance evaluation in the presence of other attacks such as cropping and logo insertion.

References:

1. C. Shoemaker, "Hidden Bits: A Survey of Techniques for Digital Watermarking," 2002.
2. D. DeMenthon and D. Doermann, "Video retrieval using spatio-temporal descriptors,"Proceedings of the eleventh ACM international conference on Multimedia pp. 508-517, 2003.
3. J. Oostveen, T. Kalker, and J. Haitsma, “Feature extraction and a database strategy for video fingerprinting,” LNCS 2314, pp. 117–128, 2002.
4. Kahate A., “CRYPTOGRAPHY AND NETWORK SECURITY”, Tata-McGraw-Hill, 2nd edition (2008).
5. M. K. Mihcak and R. Venkatesan, "Video Watermarking Using Image Hashing,"
6. Microsoft Research Technical Report vol. 14, p. 19, 2001.
7. Petkovic, M., Jonker, W. Preface, “Special issue on secure data management,” Journal of Computer Security, 17(1), pp.1-3 (2009).
8. ReefVid: Free Reef Video Clip Database [Online]. Available: http://www.reefvid.org.
9. Rubata Riasat, Imran Sarwar Bajwa, M. Zaman Ale “A Hash-Based Approach for Colour Image Steganography” 978-1-61284-941-6/11/$26.00 ©2011 IEEE.